What is claimed is:

Sub a1

1. A system for authenticating message data to be exchanged between a sender and a receiver, comprising:

a controller that dynamically selects one of a plurality of authentication mechanisms to be used in providing authentication for an exchange of message data;

a security association and key management module that establishes security associations for said plurality of authentication mechanisms; and

an authentication module that includes support for said plurality of authentication mechanisms, wherein said authentication module generates an authentication tag using an authentication mechanism selected by said control, said authentication tag being appended to said message data.

2. The system of claim 1, wherein said controller receives an input identifying a processor load.

3. The system of claim 1, wherein said controller receives an input identifying an authentication error level.

4. The system of claim 1, wherein said controller receives an input identifying network defense alarms.

5. The system of claim 1, wherein said controller receives an input identifying a security policy.

6. The system of claim 1, wherein said controller includes a network security service resource and one or more security association resource managers contexts, each of said one or more security resource managers contexts being established for a corresponding network application and being responsible for establishing and maintaining an authentication mechanism for a corresponding associated network application, said network security service resource being responsible for providing resource and security constraints within which each of said one or more security resource managers contexts operates.

7. The system of claim 1, wherein said security association and key management module generates an authentication key for authenticating said message data.

8. The system of claim 1, wherein said security association and key management module generates a confidentiality key for securing control messages.

9. The system of claim 1, wherein said security association and key management module operates in accordance with the Internet Key Exchange standard.

10. The system of claim 1, wherein said authentication module operates in accordance with the IPsec standards.

11. A system for authenticating message data to be exchanged between a sender and a receiver, comprising:

a controller that dynamically selects one of a plurality of authentication mechanisms to be used in providing authentication for an exchange of message data; and

an authentication module that generates an authentication tag using said selected authentication mechanism, said authentication tag being appended to said message data.

12. The system of claim 1, further comprising a security association and key management module that establishes and maintains said plurality of authentication mechanisms.

13. The system of claim 2, wherein said security association and key management module operates in accordance with IKE.

14. A method for authenticating information to be exchanged between a sender and a receiver, comprising:

(a) identifying a change in a parameter that affects a selection of an authentication strength level between a sender and a receiver; and

(b) dynamically modifying said authentication strength level based upon said identified change.

15. The method of claim 14, wherein step (a) comprises identifying a change in processor load.

16. The method of claim 14, wherein step (a) comprises identifying a change in authentication error level.

17. The method of claim 14, wherein step (a) comprises receiving a network defense alarm.

18. The method of claim 14, wherein step (a) comprises identifying a change in security policy.

19. A method for authenticating information to be exchanged between a sender and a receiver, comprising:

(a) selecting a first authentication mechanism from among a plurality of authentication mechanisms that collectively define at least two different authentication strength and performance tradeoffs; and

(b) dynamically switching from said first authentication mechanism to a second authentication mechanism in said plurality of authentication mechanisms in response to a change in a monitored condition.

20. The method of claim 19, wherein step (b) comprises switching to said second authentication mechanism upon a change in processor load.

21. The method of claim 19, wherein step (b) comprises switching to said second authentication mechanism upon a change in authentication error level.

22. The method of claim 19, wherein step (b) comprises switching to said second authentication mechanism upon receipt of a network defense alarm.

23. The method of claim 19, wherein step (b) comprises switching to said second authentication mechanism upon a change in security policy.